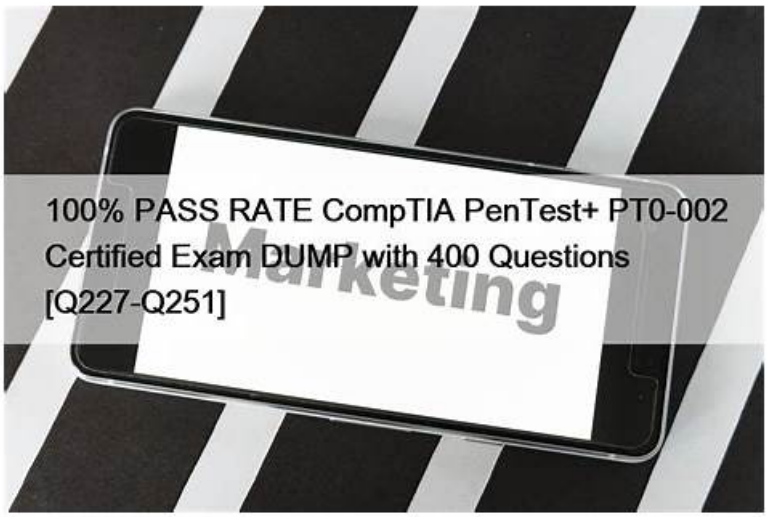
PT0-002 Exam Braindumps | Valid PT0-002 Exam Sample



BONUS!!! Download part of TestBraindump PT0-002 dumps for free: https://drive.google.com/open?id=15VuRecVRK_drYfiREhZ4PDrmhplx5iNI

TestBraindump is obliged to give you three months of free update checks to ensure the validity and accuracy of the CompTIA PenTest+ Certification (PT0-002) exam dumps. We also offer you a 100% money-back guarantee, in the very rare case of failure or unsatisfactory results. This puts your mind at ease when you are CompTIA PenTest+ Certification (PT0-002) exam preparing with us.

The PT0-002 exam consists of multiple-choice and performance-based questions that test the candidates' theoretical knowledge and practical skills in penetration testing. PT0-002 exam is 165 minutes long and comprises 85 questions. The passing score is 750 out of 900 points, and the exam fee is $359 USD. CompTIA recommends that candidates have at least two years of hands-on experience in the field of cybersecurity, including penetration testing, before taking the exam.

CompTIA PenTest+ certification exam, also known as PT0-002, is designed for ethical hackers and penetration testers who want to validate their knowledge and skills in identifying and addressing vulnerabilities in network infrastructures, web applications, and wireless networks. The CompTIA PT0-002 Certification Exam is an updated version of the previous PT0-001 exam and covers the latest industry best practices and techniques used by cybersecurity professionals to assess and secure modern network infrastructures.

>> PT0-002 Exam Braindumps <<

Trusted PT0-002 Exam Braindumps | Easy To Study and Pass Exam at first attempt & Useful CompTIA CompTIA PenTest+ Certification

To find the perfect PT0-002 practice materials for the exam, you search and re-search without reaching the final decision and compare advantages and disadvantages with materials in the market. With systemic and methodological content within our PT0-002 practice materials, they have helped more than 98 percent of exam candidates who chose our PT0-002 guide exam before getting the final certificates successfully.

CompTIA PenTest+ Certification Sample Questions (Q146-Q151):

NEW QUESTION # 146
A penetration tester executes the following Nmap command and obtains the following output:

Which of the following commands would best help the penetration tester discover an exploitable service?

A)

B)

C)

D)

- A. nmap -v -- script=mysql-info.nse remotehost
- B. nmap --ocript=omb-brute.noe remotehoat
- C. nmap -v -p 25 -- soript smtp-enum-users remotehost
- D. nmap -p 3306 -- script "http*vuln*" remotehost

Answer: A

Explanation:
The Nmap command in the question scans all ports on the remote host and identifies the services and versions running on them. The output shows that port 3306 is open and running MariaDB, which is a fork of MySQL.
Therefore, the best command to discover an exploitable service would be to use the mysql-info.nse script, which gathers information about the MySQL server, such as the version, user accounts, databases, and configuration variables. The other commands are either misspelled, irrelevant, or too broad for the task. References: Best PenTest+ certification study resources and training materials, CompTIA PenTest+ PT0-002 Cert Guide, 101 Labs - CompTIA PenTest+: Hands-on Labs for the PT0-002 Exam

NEW QUESTION # 147
A penetration tester captured the following traffic during a web-application test:

Which of the following methods should the tester use to visualize the authorization information being transmitted?

- A. Decrypt the authorization header using bcrypt.
- B. Decode the authorization header using Base64.
- C. Decrypt the authorization header using AES.
- D. Decode the authorization header using UTF-8.

Answer: B

NEW QUESTION # 148
Performing a penetration test against an environment with SCADA devices brings additional safety risk because the:

- A. devices are obsolete and are no longer available for replacement.
- B. devices may cause physical world effects.
- C. devices produce more heat and consume more power.
- D. protocols are more difficult to understand.

Answer: D

NEW QUESTION # 149
A penetration tester is conducting an assessment against a group of publicly available web servers and notices a number of TCP resets returning from one of the web servers. Which of the following is MOST likely causing the TCP resets to occur during the assessment?

- A. The local antivirus on the web server Is rejecting the connection.
- B. The web server is redirecting the requests.
- C. The web server is using a WAF.
- D. The web server is behind a load balancer.

Answer: C

Explanation:
Explanation
A Web Application Firewall (WAF) is designed to monitor, filter or block traffic to a web application. A WAF will monitor incoming and outgoing traffic from a web application and is often used to protect web servers from attacks such as SQL Injection, Cross-Site Scripting (XSS), and other forms of attacks. If a WAF detects an attack, it will often reset the TCP connection, causing the connection to be terminated. As a result, a penetration tester may see TCP resets when a WAF is present. Therefore, the most likely reason for the TCP resets returning from the web server is that the web server is using a WAF.

NEW QUESTION # 150
During enumeration, a red team discovered that an external web server was frequented by employees. After compromising the server, which of the following attacks would best support ----------company systems?

- A. A watering-hole attack
- B. A cross-site scripting attack
- C. A command injection attack
- D. Aside-channel attack

Answer: A

Explanation:
The best attack that would support compromising company systems after compromising an external web server frequented by employees is a watering-hole attack, which is an attack that involves compromising a website that is visited by a specific group of users, such as employees of a target company, and injecting malicious code or content into the website that can infect or exploit the users' devices when they visit the website. A watering-hole attack can allow an attacker to compromise company systems by targeting their employees who frequent the external web server, and taking advantage of their trust or habit of visiting the website. A watering-hole attack can be performed by using tools such as BeEF, which is a tool that can hook web browsers and execute commands on them2. The other options are not likely attacks that would support compromising company systems after compromising an external web server frequented by employees. A side-channel attack is an attack that involves exploiting physical characteristics or implementation flaws of a system or device, such as power consumption, electromagnetic radiation, timing, or sound, to extract sensitive information or bypass security mechanisms. A command injection attack is an attack that exploits a vulnerability in a system or application that allows an attacker to execute arbitrary commands on the underlying OS or shell. A cross-site scripting attack is an attack that exploits a vulnerability in a web application that allows an attacker to inject malicious scripts into web pages that are viewed by other users.

NEW QUESTION # 151
.....

Our CompTIA PenTest+ Certification study questions have a high quality, that mainly reflected in the passing rate. More than 99% students who use our PT0-002 exam material passed the exam and successfully obtained the relating certificate. This undoubtedly means that if you purchased PT0-002 exam guide and followed the information we provided you, you will have a 99% chance of successfully passing the exam. So our PT0-002 study materials are a good choice for you. In order to gain your trust, we will provide you with a full refund commitment. If you failed to pass the exam after you purchase PT0-002 Exam Material, whatever the reason, you just need to submit your transcript to us and we will give you a full refund. We dare to make assurances because we have absolute confidence in the quality of CompTIA PenTest+ Certification study questions. We also hope you can believe that PT0-002 exam guide is definitely the most powerful weapon to help you pass the exam.

Valid PT0-002 Exam Sample: https://www.testbraindump.com/PT0-002-exam-prep.html

- Book PT0-002 Free □ PT0-002 Updated CBT □ Actual PT0-002 Test Answers □ Easily obtain free download of ▷ PT0-002 ◁ by searching on ☀ www.testsimulate.com □☀□ □Latest PT0-002 Exam Pass4sure
- CompTIA PT0-002 PDF Dumps - The Fastest Way To Prepare For Exam □ Easily obtain free download of □ PT0-002 □ by searching on " www.pdfvce.com " □Exam PT0-002 Questions Answers
- New PT0-002 Dumps Ebook □ Valid PT0-002 Exam Dumps □ PT0-002 Examcollection Questions Answers □ Download ➥ PT0-002 □ for free by simply searching on □ www.pass4leader.com □ □PT0-002 Examcollection
- PT0-002 Exam Exam Braindumps - Newest Valid PT0-002 Exam Sample Pass Success □ Search for 《 PT0-002 》 and download it for free immediately on □ www.pdfvce.com □ □PT0-002 Test Study Guide
- PT0-002 Free Sample □ PT0-002 Latest Exam Cost □ Reliable PT0-002 Test Practice □ Open website ✔ www.prep4away.com □✔□ and search for { PT0-002 } for free download □PT0-002 New Dumps Ppt
- PT0-002 Latest Exam Cost □ Valid PT0-002 Exam Dumps □ PT0-002 Vce Format □ Open website □ www.pdfvce.com □ and search for ☀ PT0-002 □☀□ for free download □Valid PT0-002 Exam Dumps
- CompTIA PT0-002 PDF Dumps - The Fastest Way To Prepare For Exam □ Copy URL ✔ www.prep4away.com □✔□ open and search for 「 PT0-002 」 to download for free □PT0-002 Updated CBT
- Free 1 year CompTIA PT0-002 Dumps Updates □ Go to website □ www.pdfvce.com □ open and search for （ PT0-002 ） to download for free □PT0-002 New Dumps Ppt
- Reliable PT0-002 Test Simulator □ Latest PT0-002 Exam Cost □ PT0-002 Examcollection □ The page for free download of ➤ PT0-002 □ on ➥ www.torrentvalid.com □ will open immediately □Actual PT0-002 Test Answers
- PT0-002 Cost Effective Dumps □ PT0-002 New Dumps Ppt □ PT0-002 Latest Exam Cost □ Search for ▶ PT0-002 ◀ on " www.pdfvce.com " immediately to obtain a free download □PT0-002 Training Materials
- Exam PT0-002 Questions Answers □ Actual PT0-002 Test Answers □ PT0-002 Updated CBT ۞ Open 「 www.passcollection.com 」 and search for [PT0-002] to download exam materials for free □PT0-002 Examcollection
- apexeduinstitute.com, www.xiaomibbs.com, tahike9295.gynoblog.com, www.stes.tyc.edu.tw, ncon.edu.sa, sahabatperawat.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bicyclebuysell.com, Disposable vapes

2025 Latest TestBraindump PT0-002 PDF Dumps and PT0-002 Exam Engine Free Share: https://drive.google.com/open?id=15VuRecVRK_drYfiREhZ4PDrmhplx5iNI